PERFORMANT

August 11, 2017

SAMPLE LETTER
SAMPLE ADDRESS
SAMPLE CITY, ST ZIP

NOTICE OF DATA BREACH

Dear SAMPLE:

We are writing to you because of a recent information security incident at Campbell Taylor & Company ("C&T"), a certified public accountant and consulting firm that provides services to Performant Financial Corporation ("Company" or "Performant") as an external auditor. This incident involved the possible exposure of personal information for certain current and former Performant employees related to Performant's 401K plan. As a result, please see the following important information.

What Happened?

By letter dated April 7, 2017, C&T informed Performant that after noticing unusual activity on its network, C&T had hired a specialist forensic information technology firm to investigate. As a result of that investigation it was determined that an unauthorized individual had accessed a C&T network drive between January 27, 2017, and February 2, 2017. C&T, however, could not determine whether any specific files were accessed. The network drive, unfortunately, contained the Company's 401K audit files for certain years.

Upon receiving C&T's notification of a potential data breach, Performant undertook its own investigation to determine what specific information may have been compromised. Performant attempted multiple times to obtain specific answers and definitive records from C&T to accurately determine whose information may have been compromised. Performant also attempted to gain details regarding C&Ts incident notification procedure, including information about C&T's notification to employees of its client's employees, such as Performant's employees participating in the Company's 401K plan. On June 27, 2017, C&T, for the first time, provided Performant with access to the Company's specific files stored on the C&T network drive that was compromised. After receiving the files, Performant engaged in a detailed review to determine what, if any, personal information of its current or former employees was potentially compromised. The review revealed that your information may have been compromised by the incident at C&T.

What Information Was Involved?

Although C&T cannot determine whether or not Performant's files were accessed by the unauthorized individual, the security incident may have involved your first name, last name, date of birth, and Social Security number, as a result of your participation in the Company's 401K plan in the years of 2010, 2011, and/or 2015. Please note that the data files related to this incident did not include other information about the 401K plan or information about your personal 401K, such as account access information or account balances.

What We Are Doing.

C&T has reported to us that it notified the Federal Bureau of Investigation, Internal Revenue Service, the California Franchise Tax Board, all three nationwide credit bureaus, and relevant state agencies of the incident. C&T has assured Performant that C&T has reviewed its policies and procedures, and put certain new controls in place to prevent an incident like this one from happening again in the future. We are reviewing the modifications to C&T's practices to ensure the security of Performant's (and by extension your) information in engagements with C&T. Performant has not delayed providing you with this notice as a result of a request from law enforcement.

As of the date of this letter, Performant has not received any information suggesting that your personal information has been accessed or misused. Nevertheless, and out of an abundance of caution, Performant is ensuring that you receive, at no cost to you, the 12 months of complimentary identity protection services through AllClearID that C&T has made available to other potentially affected individuals.

You have the option to use two different products through AllClear ID that are available to you as of the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Report: If you suspect that you have been victimized by identity theft, you can call AllClear Identity Repair at **1-855-861-4034** and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition. No enrollment is required to take advantage of AllClear Identity Repair. You can find the complete AllClear Identity Repair Terms of Use Here: https://www.allclearid.com/repair-terms-of-use/

AllClear Credit Monitoring: This product offers additional layers of protection which include 12months of credit monitoring and a $1 million identity theft insurance policy, at no cost to you. Details of the insurance policy can be found at https://www.allclearid.com/insurance. To enroll in credit monitoring, please follow the steps below:

- **Visit** the AllClearID website to enroll: enroll.allclearid.com
- **Provide** your redemption code: **[Redemption Code]**

Your redemption code expires **August 31, 2018**. Please note: Additional steps may be required by you in order to activate alerts and monitoring options.

If you have questions, need assistance with Identity Repair, or would like an alternative to enrolling in AllClear Credit Monitoring online, please contact AllClearID's customer care team at **1-855-861-4034.**
.

What You Can Do.

In addition to arranging for one year of free identity protection, we have included with this letter additional information on steps you can take to protect the security of your personal information. We urge you to review this information carefully.

In addition, in the unlikely case that you used your Social Security number, or some derivative of it, as a password for online access to your 401K account, you should change your password. Information concerning how you can modify your 401K account password can be found at www.401k.com and 800-890-4015.

Other Important Information.

Contact information for the entity that experienced the security breach:
Campbell Taylor & Company,3741 Douglas Blvd, Suite 350, Roseville, CA 95661; phone: 916-929-3680.

We sincerely apologize and regret any inconvenience or concern this Campbell Taylor & Company incident may cause you. Should you have any questions regarding this matter, please do not hesitate to contact us at 925-960-4965, humanresources@performantcorp.com or by mail at 333 North Canyons Parkway, Livermore, CA 94551, Attention: Human Resources 401K.

Sincerely,

Julie Snyder
Sr. Director, Human Resources

Enclosure: Steps to Protect the Security of Your Personal Information

Steps To Protect The Security Of Your Personal Information

By taking the following steps, you can help reduce the risk that your personal information may be misused.

1. Enroll in the All Clear program. If you have questions about the product, need assistance with identity repair that arose as a result of this incident or would like an alternative to enrolling in AllClear ID online, please contact AllClearID at 855-434-8077. See the enclosed 'AllClear Identity Repair Terms of Use' and their website at www.allclearid.com/personal/services/.

2. Review your credit reports. You can receive free credit reports by placing a fraud alert. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three national credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months.

3. Review your account statements. You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities and other service providers.

4. Remain vigilant and respond to suspicious activity. If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to AllClear ID before your redemption code expires.

If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. You also should consider reporting such activity to your local police department, your state's attorney general, and the Federal Trade Commission.

5. Consider placing a fraud alert with one of the three national credit bureaus. You can place an initial fraud alert by contacting one of the three national credit bureaus listed below. For 90 days, an initial fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit. If you decide to enroll in AllClear ID, you should place the fraud alert after enrolling. The contact information for all three bureaus is as follows:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, Georgia 30374	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

6. Consider Placing A Security/Credit Freeze On Your Account. You can place a security/credit freeze on your credit reports so that the three national credit bureaus will not release information about your credit without your express authorization. This means that your credit file cannot be shared with potential creditors or other persons considering opening new accounts unless you decide to unlock your file by contacting a credit reporting agency and providing a PIN or password. Most businesses will not open credit accounts without first checking a consumer's credit history. If your credit files are frozen, even someone who has your name and Social Security number would not likely be able to get credit in your name. However, because the freeze essentially locks down your credit, it can be inconvenient for people who are simply seeking extra protection for their credit.

You may obtain a security freeze over the internet or via mail. To place a security freeze on your credit report via mail, send the following to each credit bureau: (1) your full name, with middle initial and any suffixes; (2) your Social Security number; (3) your date of birth; (4) your current address and any previous addresses for the past five years; and (5) a copy of any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. Each copy must be legible, display your name and current mailing address, and the date of issue. See the contact information for all three bureaus above in section 5.

Each credit bureau may charge a fee of between $5 and $20 depending upon your state of residence to place, lift, or remove a freeze. The fee will be waived if you are a victim of identity theft or the spouse of a victim of identity theft, and submit a valid police report relating to the identity theft incident to the bureau.

7. Reporting Law Enforcement & Obtaining A Police Report. You can report an identity theft incident to local law enforcement in the county where you reside and receive a police incident report.

8. Rights under the Fair Credit Reporting Act. You have rights under the Fair Credit Reporting Act. If you are the victim of identity theft and you notify a consumer reporting agency of a misstatement in your credit report which resulted from the theft, the consumer reporting agency has an obligation to block the reporting of such information from your credit report.

9. Additional Information. You can obtain additional information about steps you can take to avoid identity theft and report suspected identity theft through the Federal Trade Commission (FTC).

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.ftc.gov/bcp/edu/microsites/idtheft/
(877) IDTHEFT (438-4338)
TDD: (866) 653-4261

If you live in Maryland, please read the additional notice below that applies to you:
For Maryland Residents:
You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov

If you live in Massachusetts, please read the additional notice below that applies to you:
For Massachusetts Residents:
Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

In order to request a security freeze, you will need to provide the following information: (i) your full name; (ii) social security number; (iii) date of birth; (iv) if you have moved in the past five years, the addresses where you have lived over the prior five years; (v) proof of current address; (vi) a legible photocopy of a government issued identification card; (vii) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and (viii) if you are not a victim of identity theft, include a $5 payment to place a security freeze.

If you live in North Carolina, please read the additional notice below that applies to you:
For North Carolina Residents:
You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

North Carolina Attorney General
Department of Justice
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-6400
http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx